

## UNITED STATES DISTRICT COURT

for the

Western District of New York

In the Matter of the Seizure of  
 (Briefly describe the property to be seized)  
 ALL VIRTUAL CURRENCY STORED  
 WITHIN, OR ASSOCIATED WITH,  
 BINANCE ACCOUNT USER ID 19925727

POPEYETOOLS.COM

POPEYETOOLS.CO.UK, and

POPEYETOOLS.TO

Case No. 24-MC-

40



**APPLICATION FOR A WARRANT  
 TO SEIZE PROPERTY SUBJECT TO FORFEITURE**

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the above-captioned Binance account, is subject to forfeiture to the United States of America under 18 U.S.C. §§ 981(a)(1)(C) and 982(a)(2)(B), and 28 U.S.C. § 2461(c); and the above captioned domain names are subject to forfeiture to the United States of America under 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B) and 1029(c)(1)(C), and 28 U.S.C. § 2461(c).

This application is based on facts set forth in the attached affidavit of Special Agent Jordan F. Slavik of the Federal Bureau of Investigation, incorporated by reference herein.

☒ Continued on the attached sheet.

Applicant's signature

Jordan F. Slavik, FBI Special Agent

Printed name and title

This application is submitted by e-mail in .pdf format and attested to me and before me as true and accurate by telephone consistent with Fed.R.Crim P.4.1 and 41(d)(3).

Date: November 15, 2024

Judge's signature

City and state: Buffalo, New York

Hon. H. Kenneth Schroeder, Jr., U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF NEW YORK

---

IN THE MATTER OF THE SEIZURE OF:

ALL VIRTUAL CURRENCY STORED WITHIN,  
OR ASSOCIATED WITH, BINANCE  
ACCOUNT USER ID 19925727

24-MC- 40

POPEYETOOLS.COM;

POPEYETOOLS.CO.UK; AND

POPEYETOOLS.TO

---

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEIZURE WARRANTS**

STATE OF NEW YORK     )  
COUNTY OF ERIE        )     ss.:  
CITY OF BUFFALO        )

**INTRODUCTION**

I, Jordan F. Slavik, being duly sworn, hereby declare as follows:

**AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since September 2019. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York, where I work on investigations relating to criminal and national security cyber intrusions. These investigations specifically focus on unlawful computer access, nefarious online marketplaces, phishing activity, and online sexual extortions. I have gained experience through numerous FBI, government, and private sector trainings and certifications, such as multiple certificates through the FBI's Advanced Cyber Training Program and cryptocurrency training curriculum; the Department of Homeland Security's Cybersecurity for Industrial Control Systems certificate; certificates from SANS on

Cyber Security essentials, Hacking Tools, and Open Source Cyber Investigations; and certificates from Mandiant on the Cybersecurity Intelligence Cycle; as well as through everyday work related to these types of investigations. Through my work in cyber-related investigations, I am familiar with the fundamental operations of the internet, hardware, and software, and the communication protocols across each. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

2. The background and facts set forth in the Affidavit supporting the Criminal Complaint filed under docket 24-MJ-5181 (W.D.N.Y.) (the “Criminal Complaint Affidavit”) are fully incorporated herein and attached hereto as Exhibit 1. The facts in this affidavit and in Exhibit 1 come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrants and does not set forth all of my knowledge about this matter. This affidavit is made in support of the issuance of criminal and civil seizure warrants for:

- (A) **Attachment A-1:** all cryptocurrencies stored within or associated with Binance User ID 19925727, including all First Digital USD, Bitcoin, Litecoin, Ethereum, TetherUS, BNB, NEO, Tokocrypto, and Gravity, approximately \$239,774.26 worth of cryptocurrency assets (the “SUBJECT CRYPTOCURRENCIES”), at the centralized virtual currency exchange (“VCE”) Binance (the “SUBJECT BINANCE ACCOUNT”); and
- (B) **Attachment A-2:** the following domain names (hereinafter referred to as the “SUBJECT DOMAIN NAMES”):

- i. popeyertools.com,
- ii. popeyertools.co.uk, and
- iii. popeyertools.to

3. As set forth in this affidavit, there is probable cause to believe that the SUBJECT CRYPTOCURRENCIES and SUBJECT DOMAIN NAMES are property constituting or derived from proceeds of access device fraud and conspiracy to commit access device fraud, in violation of Title 18, United States Code, Sections 1029(a)(2), 1029(a)(6) and 1029(b) (the “SUBJECT OFFENSES”) and therefore are subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(B), and Title 28, United States Code, Section 2461(c). Furthermore, there is probable cause to believe that the SUBJECT DOMAIN NAMES are the personal property of Abdul Sami, also known as “James Thomas,” (hereinafter, “SAMI”), used or intended to be used, to commit or facilitate the SUBJECT OFFENSES, and therefore are also subject to seizure and forfeiture pursuant to Title 18, United States Code, Section 1029(c)(1)(C).

4. Pursuant to Title 18, United States Code, Section 981(b) and Title 21, United States Code, Section 853(f), this Court is empowered to issue criminal and civil seizure warrants for the SUBJECT CRYPTOCURRENCIES and SUBJECT DOMAIN NAMES.

#### **RELEVANT STATUTORY AUTHORITY**

5. The following legal statutes will be discussed throughout this affidavit:

**Title 18, United States Code, Section 1029** provides in relevant part:

(a) Whoever-- . . .

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating \$1,000 or more during that period; . . .[and]

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b) . . .

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) Penalties.—

(1) Generally.—The punishment for an offense under subsection (a) of this section is . . . (C). . . forfeiture to the United States of any personal property used or intended to be used to commit the offense.

(2) Forfeiture procedure.—

The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act [(Title 21, United States Code, Section 853)], except for subsection (d) of that section.

**Title 18, United States Code, Section 982(a)(2)** provides in relevant part:

The court, in imposing sentence on a person convicted of a violation of, or a conspiracy to violate— . . .

(B) section . . . 1029, . . . of this title,

shall order that the person forfeit to the United States any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation.

**Title 18, United States Code, Section 981(a)(1)(C)** provides in relevant part, the following is subject to forfeiture:

(C) Any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of...any offense constituting “specified unlawful activity” (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense;

**Title 18, United States Code, Section 1956(c)(7)(D)** provides in relevant part that offenses under Title 18, United States Code, Section 1029, are considered “specified unlawful activity” (“SUA”).

**Title 28, United States Code, Section 2461(c)** provides in relevant part:

If a person is charged in a criminal case with a violation of an Act of Congress for which the civil or criminal forfeiture of property is authorized...the court shall order the forfeiture of the property as part of the criminal case pursuant to the Federal Rules of criminal Procedure and section 3554 of Title 18 United States Code.

**Title 21 United States Code, Section 853(f)** provides in relevant part:

**Warrant of seizure**

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

**Title 18, United States Code, Section 981(b)(1)** authorizes seizures or property subject to civil forfeiture based upon a warrant supported by probable cause.



**Title 18, United States Code, Section 981(b)(2)** provides in relevant part:

Seizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure . . . .

**Fed. R. Crim. P. 41** provides in relevant part:

(c) PERSONS OR PROPERTY SUBJECT TO SEARCH OR SEIZURE. A warrant may be issued for any of the following:

- (1) evidence of a crime;
- (2) contraband, fruits of crime, or other items illegally possessed;
- (3) property designed for use, intended for use, or used in committing a crime; or
- (4) a person to be arrested or a person who is unlawfully restrained

#### **BACKGROUND ON CRYPTOCURRENCY ACCOUNTS AND TRACING**

6. Based on my training and experience and information learned from others, I am aware of the following:

7. Virtual Currency: Virtual currencies are digital tokens of value circulated over the Internet. Virtual currencies are typically not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Different virtual currencies are currently in circulation. Bitcoin (or BTC) and Ether (ETH) are currently the most well-known virtual currencies in use. BTC exists on the Bitcoin blockchain and ETH exists on the Ethereum network. Typically, a virtual currency that is “native” to a particular blockchain cannot be used on a different blockchain. For instance, ETH (the native token on the Ethereum network) cannot be used on other networks unless it is “wrapped” by smart contract code.

8. Stablecoins: Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. Stablecoins achieve their price stability via collateralizations (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. First Digital USD is an example of a stablecoin pegged to the U.S. dollar.

9. Tether (USDT): Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT, another stablecoin pegged to the U.S. dollar. Other stablecoins backed by the United States dollar include USDC and DAI.

10. Virtual Currency Address: Virtual currency addresses are the virtual locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

11. Private Keys: Each virtual currency address is controlled using a unique corresponding private key, a cryptographic equivalent of a password, which is needed to access the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

12. Virtual Currency Wallet: There are various types of virtual currency wallets, including software wallets, hardware wallets, and paper wallets. The virtual currency wallets at issue for the purposes of this affidavit are software wallets (i.e., a software application that interfaces with the virtual currency's specific blockchain and generates and stores a user's addresses and private keys). A virtual currency wallet allows users to store, send, and receive



virtual currencies. A virtual currency wallet can hold many virtual currency addresses at the same time.

13. Wallets that are hosted by third parties are referred to as “hosted wallets” because the third party retains a customer’s funds until the customer is ready to transact with those funds. Conversely, wallets that allow users to exercise total, independent control over their funds are often called “unhosted” wallets.

14. Blockchain: Many virtual currencies publicly record all of their transactions on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by the decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain’s technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

15. Blockchain Explorer: These explorers are online tools that operate as a blockchain search engine allowing users the ability to search for and review transactional data for any addresses on a particular blockchain. A blockchain explorer is software that uses application programming interface (API) and blockchain nodes to draw data from a blockchain and uses a database to arrange and present the data to a user in a searchable format. An API is a set of definitions and protocols for building and integrating application software.

16. Smart Contracts: Smart contracts are computer programs stored on a blockchain that run when predetermined conditions are met. Typically, they are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement. The Ethereum network is designed and functions based on smart contracts.

17. Virtual Currency Bridge: A blockchain bridge, otherwise known as a cross-chain bridge, connects two blockchains and allows users to send virtual currency from one chain to the other.

18. Virtual Currency Exchanges (VCEs): VCEs, such as Binance and MEXC, are trading and/or storage platforms for virtual currencies (e.g., BTC and ETH). There are generally two types of VCEs: centralized exchanges and decentralized exchanges, which are also known as "DEXs." Binance and MEXC are centralized exchanges. Many VCEs also store their customers' virtual currency in virtual currency wallets. As previously stated, these wallets can hold multiple virtual currency addresses associated with a user on a VCE's network. Because VCEs act as money services businesses, they are legally required to conduct due diligence of their customers (i.e., Know Your Customer (KYC) checks) and to have anti-money laundering programs in place (to the extent they operate and service customers in the United States).

19. Blockchain Analysis: As previously stated, while the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain (e.g., the Bitcoin blockchain). This analysis can be invaluable to criminal investigations for many reasons,

including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement uses reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

20. The analysis can also reveal additional addresses controlled by the same individual or entity. “For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (i.e., a “cluster”). It is possible to identify a ‘cluster’ of [BTC] addresses held by one organization by analyzing the [BTC] blockchain’s transaction history. Open source tools and private software products can be used to analyze a transaction.” *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

21. The third-party blockchain-analysis software utilized in this case is an anti-money laundering software provided by Company A. Among other things, Company A’s software employs a “clustering” process to identify addresses that are managed by the same individual entity and should therefore be grouped together in a “cluster.” This software is used by financial institutions and law enforcement organizations worldwide, supported many law enforcement investigations and been referenced in numerous search and seizure warrants, and as such, has been found to be reliable. Law enforcement has been able to verify the reliability of this software by ex-post analysis. For example, in an unrelated case where the government used Company A’s clustering software, the government’s blockchain analysis identified over 50 customers of a darknet child pornography site. In each one of the 50

subsequent law enforcement actions, the blockchain analysis was corroborated by statements and search warrant returns from the targets' devices. In sum, this software has correctly analyzed data on the blockchain in hundreds of investigations, and I have assisted or been briefed on many of these investigations.

22. Change Wallets: One way to identify clusters of related Bitcoin addresses is through the shared use of "change wallets." As background, an individual who seeks to send Bitcoin to a recipient wallet address often sends more Bitcoin than the person intends to ultimately transfer because of Bitcoin's protocols, which require a certain amount of data be sent for the transaction to occur. For example, if person A seeks to send \$75 worth of Bitcoin to the recipient wallet address of person B, person A may actually transmit \$100 worth of Bitcoin. Of this \$100 in bitcoin, \$75 will be sent to person B's recipient wallet address while the remaining \$25 will be sent back to person A – either to their original sending wallet address or to another wallet address in their control that is commonly referred to as a "change wallet." This operation is functionally analogous to a transaction where a person uses a \$5 bill to purchase a \$4 coffee from that coffee shop. In that example, \$4 would remain with the cashier while \$1 would be returned to the customer. In this way, when a change wallet is different than the original wallet used to send a Bitcoin payment, it is reasonable to conclude that both wallets are controlled by the same person or persons acting in concert with each other.

### **BACKGROUND ON DOMAIN NAMES**

23. Based on my training and experience, and information learned from others, I am aware of the following:

24. Internet Protocol Address: An Internet Protocol address (“IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 123.45.67.89). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address -- it enables computers connected to the Internet to properly route traffic to each other. The system of IP addresses is managed by the Internet Corporation For Assigned Names and Numbers (“ICANN”), together with five Regional Internet Registries (essentially, one for each populated continent except Australia, which is combined with most of Asia), including the American Registry for Internet Numbers (“ARIN”), which has responsibility for North America. ARIN registers IP addresses for internet-connected computers in North America and maintains records about the registered owners for those IP addresses. ARIN-registered owners are typically large users or organizations, such as remote computing or internet service providers (*e.g.*, Comcast), who can internally assign IP addresses to computers that belong to individual subscribers.

25. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond with a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

26. Domain Name System: The domain name system (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision,

or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, the “example” second-level domain, and is the web server.

27. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses.

28. Registry: For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. For example, the registry for the “.com” and “.net” top-level domains are VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

29. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Typically, a registrar will provide a registrant with the ability to change the IP address a particular IP address resolves through an online interface. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

30. WHOIS Records: The system of IP addresses and domain names is ultimately coordinated by the ICANN. ICANN requires participants in the system (including internet registries and domain name registrars) to maintain and, in many circumstances, to make



publicly available, records identifying the registrants, or users, of the domain names and IP addresses. The resulting records are known as WHOIS records. WHOIS records typically indicate the listed identity of individuals or organizations that have registered IP addresses or domain names. These WHOIS records typically include names, contact information, and address and/or location information. The names of individual subscribers or registrants are typically unverified, but in my experience, even false names can provide useful investigative leads. For example, when two domain names were registered using the same name (even fake name), and when those domain names have any other commonalities (date of registration, domain name registrar, resolving IP address), in my training and experience those two domain names are operated by the same person or organization. In addition, e-mail addresses for registrants are often attended – even for registrants engaged in criminal activities, and even where the e-mail addresses that do not reflect the registrants’ true identities – because, even if they are concealing their identities, registrants may want to receive e-mails about their domains. In addition, based on my training and experience, and my knowledge of the system, general WHOIS location data for IP addresses is typically reliable, because the vast majority of IP addresses are registered to known internet service providers (*e.g.*, Comcast) who reliably report the locations of the servers assigned to their IP addresses, and in many cases the locations of those servers (at least at the level of cities and towns) are publicly known.

31. WHOIS: A “WHOIS” search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A WHOIS record for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a WHOIS record for the domain name XYZ.COM might list an IP address range

of 12.345.67.0- 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0- 12.345.67.99.

### **THE SUBJECT DOMAIN NAMES**

32. A search of publicly available WHOIS domain name registration records revealed that the popeyertools.com domain name was registered on or about March 14, 2016 through the registrar Namecheap, Inc., which has its headquarters at 4600 East Washington Street Suite 305, Phoenix, Arizona. The publicly available WHOIS database lists the registrant of popeyertools.com as WithheldForPrivacy. WithheldForPrivacy is an entity that allows website owners to keep their contact details private during the domain name registration process.

33. A search of publicly available WHOIS domain name registration records revealed that the popeyertools.co.uk domain name was registered on or about March 14, 2018 through the registrar Namecheap, Inc., which has its headquarters at 4600 East Washington Street Suite 305, Phoenix, Arizona. The publicly available WHOIS database lists the registrant information as “redacted for privacy.”

34. A search of publicly available WHOIS domain name registration records revealed that the popeyertools.to domain name was registered on or about November 18, 2020. The name of the registrar was listed as CloudFlare Inc, which has its headquarters in San Francisco, California. There was no available information on the registrant. CloudFlare is a reverse proxy service provider used by some cyber actors to add a layer of obfuscation to the

true IP Address of a web server hosting a nefarious marketplace, such as PopeyeTools.<sup>1</sup> Information from CloudFlare identified that the true registrar for popeyetools.to domain name is Namecheap, Inc., which has its headquarters at 4600 East Washington Street Suite 305, Phoenix, Arizona.

### **INVESTIGATION**

35. Since in or around December 2018, FBI Buffalo Cybercrimes Task Force (“BCTF”) has investigated SAMI and other administrators and users of PopeyeTools for creating, administering and using an active Clearnet website named “PopeyeTools” that is dedicated to selling access devices and other illicit goods and tools of cybercrime to its thousands of users around the world. Some of the access devices sold on PopeyeTools included bank account, credit card, and debit card numbers and associated information for conducting transactions. Since its inception, PopeyeTools has offered for sale the access devices and personally identifiable information (“PII”) of at least 227,000 individuals, including some in the Western District of New York, and generated at least \$1.7 million in revenue.

---

<sup>1</sup> Based on my training and experience investigating cybercrimes, I understand that a reverse proxy server is a type of proxy server that relays information between the web browser (client) of a user visiting a website and the web server hosting a website, like a middleman. For example, if a user accesses the website [www.example.com](http://www.example.com) and [www.example.com](http://www.example.com) utilized a reverse proxy service, the user’s computer will first send a request to the reverse proxy server, and the reverse proxy server would forward the request to [www.example.com](http://www.example.com)’s web server. The legitimate uses of a reverse proxy server include Denial of Service (DoS) attack protection, increased performance, and identity protection. In the same example, if a user performs a WhoIs lookup of the domain [www.example.com](http://www.example.com), the result would be the IP Address of the reverse proxy server, not the true IP Address of [www.example.com](http://www.example.com)’s web server.

36. PopeyeTools has been accessible through several domains since its creation, including the SUBJECT DOMAIN NAMES that continue to actively facilitate access to the PopeyeTools marketplace.

37. As further described in Exhibit 1, the Criminal Complaint Affidavit, there is probable cause to believe that SAMI and two other co-conspirators committed access device offenses arising from their roles in creating, managing and supporting PopeyeTools' operations. In particular, SAMI is charged with one count of (1) conspiracy to traffic access devices and solicit another person for the purposes of offering access devices, in violation of Title 18, United States Code, Section 1029(a)(2) and (a)(6), all in violation of Title 18, Sections 1029(b)(2) and 3559(g)(1); (2) trafficking access devices, in violation of Title 18, United States Code, Sections 1029(a)(2) and 2; and (3) solicitation of another person for the purposes of offering access devices, in violation of Title 18, United States Code, Sections 1029(a)(6) and 2.

38. As detailed below, the FBI's investigation indicates that the PopeyeTools marketplace used cryptocurrency addresses provided by CoinPayments, a cryptocurrency payment processing platform, to receive its customers' payments for the illicit goods and services that it offered. Records received from CoinPayments and Binance, as well as the FBI's analysis of the Bitcoin blockchain using Company A's clustering software, reveal that SAMI controlled a number of these CoinPayments addresses through a single CoinPayments account that, in turn, transferred approximately \$888,000 worth of Bitcoin to the SUBJECT BINANCE ACCOUNT, through a cluster of PopeyeTools-related wallet addresses. This same cluster of PopeyeTools-related wallet addresses was also used to purchase and renew some of the SUBJECT DOMAIN NAMES, as detailed below.

39. As detailed in the Criminal Complaint Affidavit and further summarized below, there is probable cause to believe that: (A) the SUBJECT CRYPTOCURRENCIES and SUBJECT DOMAIN NAMES are property constituting or derived from proceeds of the SUBJECT OFFENSES; and (B) the SUBJECT DOMAIN NAMES are personal property of SAMI, used, or intended to be used, to commit or facilitate the SUBJECT OFFENSES.

#### **A. Overview of the PopeyeTools Marketplace**

40. As further detailed in the Criminal Complaint Affidavit and below, through warrants and a mutual legal assistance (MLA) request to a trusted foreign authority, the FBI has lawfully obtained multiple forensic copies of servers that hosted the PopeyeTools website since in or around 2019, including an image taken in or around May 2023. Each of these copies contained a database storing, among other things, the registration information of PopeyeTools administrators and users, as well as records of the content posted on the PopeyeTools website and the stolen access devices offered on the platform. In or around November 2018, an FBI Undercover Employee (“UCE-1”) in the Western District of New York also created a user account on PopeyeTools and periodically visited the PopeyeTools website with an Internet browser through as recently as June 2024. Through these sources, as well as the evidence detailed below and the Criminal Complaint Affidavit, your affiant has made the following observations about the operation of PopeyeTools.

41. The PopeyeTools marketplace was organized into sections. At different times, many of the sections were devoted to soliciting for sale categories of illicit goods and PII, including, but not limited to stolen access devices, as identified in Title 18, United States Code, Section 1029(a)(1), and other illicit tools, materials, and services to support the

malicious online activity of cybercriminals. Some of the items commonly sold on the platform without authorization included card-issuer type, account number, card verification value (CVV), card expiration date, personal identification numbers (PINs), and login information for accessing the account (collectively, “payment card data”). The marketplace also sold scam websites or “kits” suited to stealing payment card data (“phish kits”), tools for sending “spam” emails to large volumes of potential victims, information for accessing computer servers or devices, and guides and tutorials for how to profit from items sold on the marketplace.

42. For instance, on or about January 9, 2023, UCE-1 reviewed PopeyeTools and observed numerous sections dedicated to the unauthorized sale of payment card data. The “Live Fullz”<sup>2</sup> section offered unauthorized payment card data for cards that were marketed as “live”—*i.e.*, could be used to conduct fraudulent transactions—at a price of approximately \$30 per card. Other sections included “Fresh Bank Logs,”<sup>3</sup> which offered logs of stolen bank account information, “Dead Fullz,”<sup>4</sup> “Fresh Leads” or email spam lists, “Scam pages,” and “Guides and Tutorials.”

---

<sup>2</sup> In my training and experience, “Fullz” is a slang term on underground carding forums that refers to packages of PII and access device information of unwitting victims. This data often contains an individual’s name, social security number, date of birth, address, and payment card data, and is offered and sold through marketplaces without the individual’s consent. Fullz can be used by malicious cyber actors to engage in fraudulent activities without that person’s consent, such as conducting unauthorized transactions with stolen payment card data or opening new financial accounts under the victim’s identity to do the same.

<sup>3</sup> According to the investigation, “Bank logs” were packages of banking information, which typically included individuals’ names, bank account numbers, and routing numbers. “Live” or “fresh” bank logs contained information for active bank accounts.

<sup>4</sup> In my training and experience, as well as the investigation, “Dead Fullz” is a slang term on underground carding forums that refers to cards that cannot be used to conduct fraudulent transactions directly. However, these cards are marketable to cybercriminals because they contain PII and other information that can be used to facilitate identity theft, bank fraud, and credit card fraud schemes.



43. PopeyeTools typically required an individual to create an account to view its marketplace. To purchase an item offered on the website, a PopeyeTools user typically needed to transmit virtual currency, such as Bitcoin, to the PopeyeTools administration to establish an account balance with the marketplace, and then select and purchase an item or item(s) from the PopeyeTools website by drawing from that account balance. At various times since its creation, the marketplace sold credit card information of individuals in the Western District of New York.

44. As further explained in the Criminal Complaint Affidavit, PopeyeTools developed and advertised tools and policies designed to entice PopeyeTools customers to use the marketplace to buy illicit goods and tools. For instance, at certain times, PopeyeTools listed the following motto next to its section headers: “We Believe in Quality Not Quantity.” PopeyeTools also promised to refund or replace purchased “Live Fullz” that were no longer valid at the time of sale and, at different times, PopeyeTools provided customers with access to services that could be used to check the validity of certain payment card data offered through the website. PopeyeTools also promoted that its users could operate anonymously on the platform. For instance, within its Frequently Asked Questions (“FAQ”) page, UCE-1 observed a “Rules” section that stated, in relevant part, “Fully secure. No logging. No IP tracking.” In context, PopeyeTools appears to have been advertising that the marketplace would not track or retain information about its customers.

45. Beyond the design and operation of the platform, the administrators of PopeyeTools also posted additional messages on the platform evidencing their knowledge and intent to facilitate the trafficking of unauthorized access devices. For instance, at different times, UCE-1 observed that the “Bank Logs” section of the FAQ page stated: “We not

responsible if owner move [sic] money after buy.” Similarly, in the “Dead Fullz” section, PopeyeTools stated that it was “not responsible for your Damage.”

46. In addition, in or around August 2018, the PopeyeTools website posted offers in the “Guides and Tutorials” section to sell items that were described as supporting carding, including “How To Cash Out From Stolen Credit Cards via Online Games,” “How To Get Unlimited Live Users and Credit Cards,” “Dumps tutorial for Beginners,”<sup>5</sup> and “How to open your OWN Bank Drops.”<sup>6</sup>

47. In the “Admin” or “Admin Contact” section of the FAQ page, the PopeyeTools website provided a means for users to contact the website. At certain times in 2019, the PopeyeTools website listed the email address PopeyeTools@gmail.com. As of at least in or around January 2023, the PopeyeTools website was updated to list messenger accounts at ICQ and Telegram, two messaging services, with the usernames “PopeyeTools.”

48. According to PopeyeTools databases, some of its user accounts were registered with email addresses known to be associated with cybercrime, including ransomware activity.

---

<sup>5</sup> In my training and experience, the term “dumps” or “dump data” are slang terms on underground carding forums that refer to the data obtained through the unauthorized copying of payment card data and other credit card information from the magnetic stripe of a payment card.

<sup>6</sup> In my training and experience, the term “drop” is a slang term on underground carding forums that refers to a location or individual able to securely receive and forward funds or goods obtained through a cashout or other types of fraud, and typically can be used to obscure or conceal fraudulent transactions.

**B. PopeyeTools' Solicitations and Sale of Access Devices**

49. As detailed further in the Criminal Complaint Affidavit, on multiple occasions between in or around 2018 and 2021, UCE-1 used an Internet browser on a computer in the Western District of New York to purchase access devices and other illicit tools offered by PopeyeTools website, including bank logs, phishing kits, and credit cards. For instance, on or about April 19, 2021, UCE-1 purchased 25 Visa-branded credit cards by transmitting Bitcoin worth approximately \$1000 USD to a particular Bitcoin address specified by PopeyeTools. The purchased payment card data included full name, date of birth, email, phone, address, card number, card expiration date, CVV, financial account number, sort code, and IP Address.

50. As noted above, and further explained in the Criminal Complaint Affidavit, the FBI has obtained multiple forensic copies of servers that hosted the PopeyeTools website from in or around 2019 through 2023 from Namecheap and Instant Dedicated B.V. ("Instant Dedicated"), which is a hosting provider located in the Netherlands. Collectively, these images included content posted on the PopeyeTools website, transaction receipts, victim information, and the stolen access devices offered on the platform. For instance, in 2019, records provided by Namecheap showed payment card data, including credit or debit card numbers, CVVs, card expiration dates, login credentials, including usernames and associated passwords, and associated account holder PII for approximately 60,000 Visa and Master Card<sup>7</sup>-branded credit cards offered for sale on PopeyeTools at the time. The data showed large

---

<sup>7</sup> In my training and experience, Visa Inc. ("Visa") and Mastercard Inc. ("Mastercard") are American multinational payment card services corporation headquartered in the United States that support Visa-branded and Master Card-branded credit cards, debit cards and prepaid cards.

volumes of credit card account holders in the United States and Europe, including credit cards issued by U.S. financial institutions. The FBI subsequently interviewed some U.S. persons whose credit cards were offered on the PopeyeTools marketplace, including K.W., E.C., C.H., and M.F., each of whom resided in the Western District of New York in 2019. The individuals in the district verified the authenticity of the payment card data posted on PopeyeTools, and confirmed that their information had been possessed and offered for sale on the marketplace without their authorization.

51. Similarly, the FBI's review of an image obtained from Instant Dedicated revealed additional data concerning the operation and use of PopeyeTools from in or around October 2017 through in or around May 2023, including additional information concerning PopeyeTools' customers, victims, and transactions. In total, the data showed that PopeyeTools had sold or offered the payment card data of at least 227,000 victims around the world, including thousands of U.S. victims, sold approximately 255,000 different products, and generated sales revenue of at least \$1,725,000.

### **C. Identification of SAMI**

52. As further detailed in the Criminal Complaint Affidavit, the FBI's review of the PopeyeTools user databases, as well as records obtained from additional accounts associated with supporting the operations of PopeyeTools, led to the identification of multiple registration email addresses for PopeyeTools administrator accounts. Court-authorized warrants to search these and related email accounts have led to the identification of several individuals involved in supporting the administration of the website, including SAMI. Collectively, these accounts show that SAMI served as an administrator of PopeyeTools who

established and supported core aspects of the marketplace's operations, including by registering hosting, domain registrar, and cryptocurrency accounts used by the platform.

53. For instance, as the Criminal Complaint Affidavit further explains, records received from NameCheap in or around January 2019 showed that the PopeyeTools.com domain was registered with the email address abdulsami\_gi@hotmail.com (SAMI EMAIL) and the subscriber phone number +923322442698 ("the 2698 Telephone Number"). Records received from Microsoft pursuant to a warrant issued in the Western District of New York revealed numerous emails linking the SAMI EMAIL with the administration of PopeyeTools. For example, the SAMI EMAIL received email confirmations and receipts for purchasing various hosting packages and services for the marketplace. From in or around June 3, 2017, through in or around January 27, 2019, the SAMI EMAIL also received over 2000 emails from CoinPayments, a cryptocurrency exchange, addressed to "PopeyeTools" that appeared to pertain to customer purchases on the marketplace. The SAMI EMAIL further received emails about login notifications to the PopeyeTools' "cPanel." Based upon my knowledge and experience, a cPanel is a type of web hosting control panel tool that allows an administrator of a website to more easily configure and monitor the website. Accordingly, in my training and experience, the types of cPanel notifications that the SAMI EMAIL received would typically only be sent to the administrator of a website.

54. In addition, the SAMI EMAIL contained substantial evidence of SAMI's real identity beyond the account's incorporation of the name "Abdul Sami" in the email address abdulsami\_gi@hotmail.com. For instance, from in or around February 2017 through in or around January 2019, the account received routine bank statements and transaction records for United Bank Ltd., a Pakistan-based bank, for an account in the name "Abdul Sami" at an

address in Karachi, Pakistan. The SAMI EMAIL likewise received emails from the cryptocurrency exchange platform Bittrex that were addressed to “Abdul Sami.” In one of these email exchanges, the SAMI EMAIL provided Bittrex with a copy of the Pakistani National Identification Card bearing the name “Abdul Sami” with a listed date of birth of October 26, 1989 and father name of “Sultan Muhammad” (“SAMI Pakistani National Identification Card”).

55. In addition, in or around August 2019, the FBI received records from CoinPayments regarding the CoinPayments account used to facilitate cryptocurrency payments to the PopeyeTools marketplace. These records showed a CoinPayments account with the username “PopeyeTools” that was registered with the SAMI Email and used PopeyeTools@gmail.com as its public email. KYC information associated with the account likewise showed that the user had provided CoinPayments a photograph of a person who appeared to be SAMI holding a Pakistani driving license in the name of “Abdul Sami.” The driver’s license listed biographical information for “Abdul Sami” that matched the information listed in the SAMI Pakistani National Identification Card.

56. Further, the email addresses PopeyeTools@gmail.com and bakrino03@gmail.com were labeled as administrator accounts in the PopeyeTools user databases obtained in 2019. As the Complaint Affidavit explains, warrants issued in the Western District of New York in or around January 2019, and again in or around August



2023, concerning both of these Google accounts revealed that the SAMI EMAIL and the 2698 Telephone Number were listed as recovery methods.<sup>8</sup>

57. In addition, records received from Google concerning the PopeyeTools@gmail.com account confirmed that it was primarily used to administer PopeyeTools and correspond with PopeyeTools customers about the sale of illicit products and associated payment processing issues. For instance, from in or around 2018 through in or around 2020, the account exchanged numerous emails with customers concerning issues with the sale of victim “Fullz” and bank account logs. Similarly, in November 2020, the account sent multiple emails to nine different email accounts who are known to be vendors on the PopeyeTools marketplace. These emails asked vendors where payment should be sent for recent items sold on the marketplace. Further, the account also exchanged emails with CoinPayments.net support concerning the use of the CoinPayments payment processing plugin tool, which the marketplace used to allow customers to use Bitcoin for purchases. The PopeyeTools@gmail.com account further contained correspondence with UCE-1 about undercover purchases of items sold through the marketplace.

58. The PopeyeTools@gmail.com account also contained evidence of it being used by “Abdul Sami” (SAMI), a 34-year-old Pakistani national. For instance, the account received approximately 100 emails addressed to an “Abdul” between in or around May 2018

---

<sup>8</sup> Based on my training and experience, I understand that a recovery email address or phone number can be used to retain control over a primary account in the event access to it is compromised or otherwise interrupted (e.g., forgotten password), and receive notifications associated with the account’s activities. As a result, in my training and experience, whoever controls the recovery email account or phone number is likely to also control the primary email account.

and in or around September 2020. The account likewise forwarded an email to abdulsami\_gi@hotmail.com. In response to a request for identity verification documents from Payoneer, a U.S. based online payment processor, the PopeyeTools@gmail.com account also sent several documents containing identity information relating to SAMI and another individual<sup>9</sup> on or about February 20, 2018.

### **THE SUBJECT DOMAIN NAMES**

59. As the Criminal Complaint Affidavit detailed, PopeyeTools has changed the domains and servers it used to host the marketplace on multiple occasions since its creation. For instance, the BCTF has observed that the content of the PopeyeTools marketplace was primarily accessible through the domain name PopeyeTools.com from in or around October 2016 through in or around June 2019, PopeyeTools.uk from in or around June 2019 through in or around December 2020, and PopeyeTools.to since in or around January 2021. Despite the changes to the website's domain names and servers, the PopeyeTools marketplace has largely remained unchanged. For example, each iteration of the PopeyeTools marketplace shared a similar structure, fonts, and administrator contact information.

60. Although the PopeyeTools website currently uses the domain PopeyeTools.to, the website's older domains (PopeyeTools.com and PopeyeTools.uk) continue to facilitate

---

<sup>9</sup> The FBI's investigation indicates that the popeyetools@gmail.com account also sent emails under the persona "Brian Tshibangu." In a parallel prosecution in the United Kingdom, an individual named Ryan Wilson, a United Kingdom national who resided in the United Kingdom, pleaded guilty to participating in cyber-enabled fraud, including working with SAMI. As part of his plea, Wilson admitted that he used the "Brian Tshibangu" persona and opened financial accounts on behalf of SAMI. Records received from Microsoft indicate that the abdulsami\_gi@hotmail.com account was only accessed from IP addresses that resolved to internet service providers in Pakistan. Accordingly, under the circumstances and my training and experience, it appears that SAMI used the Tshibangu fake persona in an effort to conceal his identity.

access to its illicit content. Notably, on multiple occasions between in or around April 2021 and on or about November 7, 2024, the BCTF has visited the PopeyeTools.com website with an Internet browser and observed that it directs Internet users to the current PopeyeTools marketplace at [www.PopeyeTools.to](http://www.PopeyeTools.to). Similarly, the BCTF has observed on multiple occasions between in or around January 2021 and on or about October 15, 2024 that the website associated with PopeyeTools.uk automatically redirects Internet users to the PopeyeTools.com website.

61. In or around October 2024, records received from Namecheap concerning the SUBJECT DOMAIN NAMES indicated that the domains [popeyetools.com](http://popeyetools.com) and [popeyetools.co.uk](http://popeyetools.co.uk) were purchased by the same Namecheap account in or around March 2016, in or around March 2018, respectively. KYC information associated with the Namecheap account listed the name “Abdul Sami,” the SAMI Email, and the 2698 Telephone Number. The records received from Namecheap further show that the account renewed its purchase of the PopeyeTools.com and PopeyeTools.co.uk on a roughly annual basis, and that payments were made in or around May 2021, in or around March 2022, in or around March 2023, and in or around February 2024. These four purchases were made using Bitcoin sent from the following Bitcoin wallet addresses (collectively, the “PopeyeTools Addresses”):

[bc1qpenkpdhrgyxfad8r6ypxwxukcjp3pr7n0yk7u](https://blockchain.info/address/bc1qpenkpdhrgyxfad8r6ypxwxukcjp3pr7n0yk7u) (May 2021);

[bc1qgee5dsm00dhwfsxzs6q4rm4qdes2ak3ypwkr0a](https://blockchain.info/address/bc1qgee5dsm00dhwfsxzs6q4rm4qdes2ak3ypwkr0a) (March 2022);

[36jmpKXvTRJUXf4pKmR4REsorAdR3DKy6P](https://blockchain.info/address/36jmpKXvTRJUXf4pKmR4REsorAdR3DKy6P) (March 2023); and

[bc1q6w8c973hagckr9g05a9jzaz59yafcuyp2mcdng](https://blockchain.info/address/bc1q6w8c973hagckr9g05a9jzaz59yafcuyp2mcdng) (February 2024).

62. In October 2024, a cryptocurrency analyst with the FBI used analytical tools provided by Company A to analyze the blockchain and determine that the PopeyeTools Addresses were part of larger group of Bitcoin wallet addresses that all were controlled by the same individual—a grouping known as a cluster (hereinafter the “PopeyeTools Cluster”). Specifically, the FBI was able to associate these Bitcoin wallet addresses together with a high degree of confidence through an analysis of the change wallet addresses used by the PopeyeTools Cluster.<sup>10</sup>

63. The FBI’s examination of a server image obtained from Instant Dedicated in or around 2023, as previously described, showed that the PopeyeTools marketplace (PopeyeTools.to) used a series of CoinPayments Bitcoin addresses to receive customer payments. Records received from CoinPayments in or around August 2024, as well as the analysis of the blockchain, revealed that these CoinPayments addresses were associated with a particular CoinPayments account (the “PopeyeTools CoinPayments Account”) that sent the PopeyeTools Cluster approximately 1,000 payments worth a total of approximately \$888,000 between on or about November 8, 2020 and on or about September 13, 2024. The records received from CoinPayments showed that the PopeyeTools CoinPayments Account was registered to “Abdul Sami” and listed SAMI’s date of birth. The account also listed the

---

<sup>10</sup> In my training and experience, when someone utilizes bitcoin to send money to a recipient wallet address, an amount of bitcoin larger than what is intended is initially sent. This is due to the bitcoin protocol requiring a certain amount of data to be sent for the transaction to occur. For example, if person A sends person B \$75 in bitcoin, the bitcoin (blockchain) protocol will actually send \$100. Of this \$100 in bitcoin, \$75 will be sent to person B’s recipient wallet address while the remaining \$25 will be sent back to person A – either to their original sending wallet address or to another wallet address in their control. Person A’s wallet address that receives this excess money back is known as a “change wallet.” This functions much the same way as a purchase at a coffee shop would if one were to purchase a coffee for \$4 and pay with a \$5 bill. \$4 would remain with the cashier while \$1 would be returned to the customer. In this way, when a change wallet is different than the original wallet used to send a bitcoin payment, it is safe to conclude that both wallets are controlled by the same person.

SAMI Email, the 2698 Telephone Number, the SAMI Karachi address, and included photographs of SAMI's Pakistani Passport and face.

64. The October 2024 records from Namecheap concerning the SUBJECT DOMAIN NAMES also indicated that the domain was purchased in or around October 2023 by a Namecheap customer utilizing the email Address: kenton.janis@apexscore.com. Based upon a WHOIS query, BCTF identified that this email was maintained by Shinjiru Inc., a Malaysia server provider. A historical WHOIS query indicates that Shinjiru has been hosting the popeyetoools.to server since in or around 2020. Records received from Google concerning the bakrino03@gmail.com email associated with SAMI likewise showed receipts of the earlier purchase of the popeyetoools.to domain and server from Shinjiru in November 2020.

65. Like other domain names, the SUBJECT DOMAIN NAMES constitute an intangible property right. That is, registration and ownership of a domain name constitutes a well-defined property interest that can be, and are, bought and sold. The registrant of the SUBJECT DOMAIN NAMES, by virtue of controlling the registration, directs where on the Internet (to which IP address and servers) users are sent when they visit the SUBJECT DOMAIN NAMES via web browser. Moreover, ownership and control of the SUBJECT DOMAIN NAMES is exclusive – others cannot direct the registrar or the registry as to what IP address/servers the SUBJECT DOMAIN NAMES should resolve (absent a seizure warrant/court order as sought here).

66. GoDaddy, a well-known registrar and internet services provider, uses an algorithm to estimate the value of domain names, an estimate which is affected by, among other things, the amount of web traffic to the domain. As GoDaddy states on its site, "We

use our exclusive algorithm that combines machine learning with years of real market sales data, to create a rock-solid starting point for future sales, trades or negotiations. This information is based on quantitative data that we've compiled from our experience as the world's largest domain registrar." On or about October 21, 2024, GoDaddy's algorithm estimated that each of the SUBJECT DOMAIN NAMES are worth between approximately \$100 and \$1400.

### **SUBJECT CRYPTOCURRENCIES**

67. As noted above, the PopeyeTools CoinPayments Account registered to SAMI transferred a total of approximately \$888,000 worth of Bitcoin to the PopeyeTools Cluster between on or about November 8, 2020 and on or about September 13, 2024. The FBI's blockchain analysis shows that the PopeyeTools Cluster then deposited approximately \$888,000 worth of Bitcoin into the SUBJECT BINANCE ACCOUNT over a series of 96 deposits between on or about December 29, 2020, and on or about September 15, 2024. In or around September 2024, records received from Binance confirmed the above transactions. As with the PopeyeTools CoinPayments Account, KYC information for the SUBJECT BINANCE ACCOUNT showed that it was registered to "Abdul Sami" and listed SAMI's date of birth. The account also listed the SAMI Email, the 2698 Telephone Number, and included photographs of SAMI's Pakistan National Identity Card and face.

68. The records received from Binance showed that the SUBJECT BINANCE ACCOUNT received a total of approximately \$1,200,000 worth of Bitcoin from the PopeyeTools Cluster from on or about December 29, 2020 through the time of law enforcement's request in or around September 2024, including the \$888,000 worth of Bitcoin



sent from the PopeyeTools CoinPayments Account. The FBI's review of the Binance records indicates that SAMI, upon receiving Bitcoin, often either withdrew the assets (e.g., converted to fiat currencies) or converted them to other cryptocurrency assets.

69. In total, the SUBJECT BINANCE ACCOUNT received approximately \$1,900,000 worth of cryptocurrencies between in or around December 2020 and September 2024. The FBI has not yet precisely determined the origins of the additional cryptocurrency (worth approximately \$700,000) that was transferred into SAMI's SUBJECT BINANCE ACCOUNT from sources other than the PopeyeTools Cluster. However, based on my review of records obtained from email accounts controlled by SAMI and co-conspirators pursuant to search warrants and 2703(d), as partly highlighted in the Criminal Complaint Affidavit, SAMI does not appear to have any legitimate sources of income outside of his role as an administrator of the PopeyeTools marketplace.

70. The records received from Binance showed that, as of on or about September 27, 2024, the SUBJECT BINANCE ACCOUNT held the following cryptocurrency assets worth approximately \$239,774.26 (previously defined as the "SUBJECT CRYPTOCURRENCIES"):

- a. First Digital USD: 220,424.80 (\$220,182.33 USD)
- b. Bitcoin: 0.16941 (\$11,113.86 USD)
- c. Litecoin: 71.2059 (\$4,932.44 USD)
- d. Ethereum: 0.82274 (\$2,186.92 USD)
- e. TetherUS: 490.7037 (\$490.70 USD)
- f. Binance Coin (BNB): 0.68967 (\$410.77 USD)

- g. NEO: 20.54 (\$222.45 USD)
- h. Tokocrypto: 486.90 (\$196.61 USD)
- i. Gravity: 4,176.46 (\$166.31 USD)<sup>11</sup>

71. These SUBJECT CRYPTOCURRENCIES are proceeds traceable to the \$888,000 worth of Bitcoin sent from the PopeyeTools CoinPayments Account to the SUBJECT BINANCE ACCOUNT.

### CONCLUSION

72. For the foregoing reasons, I submit that there is probable cause to believe that the SUBJECT CRYPTOCURRENCIES and SUBJECT DOMAIN NAMES are property constituting or derived from proceeds of the SUBJECT OFFENSES, and therefore subject to forfeiture to the United States pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(B), and Title 28, United States Code, Section 2461(c). There is also probable cause to believe the SUBJECT DOMAIN NAMES are the personal property of SAMI, used in and/or intended to be used in facilitating and/or committing the SUBJECT OFFENSES, and therefore also subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1029(c)(1)(C). Accordingly, I respectfully request that the Court issue seizure warrants for the SUBJECT CRYPTOCURRENCIES and SUBJECT DOMAIN NAMES.

73. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the SUBJECT CRYPTOCURRENCIES and SUBJECT DOMAIN NAMES for forfeiture. Without seizing the SUBJECT CRYPTOCURRENCIES, they can be easily transferred or dissipated. By seizing the SUBJECT DOMAIN NAMES and redirecting them

---

<sup>11</sup> There were additional virtual assets in the account that had values at under \$100 USD.

to another website, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the SUBJECT DOMAIN NAMES will prevent third parties from reconstituting the popeyetools.com, popeyetools.co.uk, and popeyetools.to websites in their present form.

#### **SEIZURE PROCEDURE FOR SUBJECT CRYPTOCURRENCIES**

74. Because the warrant will be served on the VCE Binance, which will then collect the funds at a time convenient to it and wire it to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

#### **SEIZURE PROCEDURE FOR SUBJECT DOMAIN NAMES**

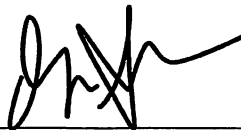
75. As detailed in Attachment A-2, upon execution of the seizure warrant, the registrar for popeyetools.com, popeyetools.co.uk, and popeyetools.to, Namecheap Inc., headquartered at 4600 East Washington Street Suite 305, Phoenix, Arizona, shall be directed to restrain and lock the SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or DOJ.

76. In addition, upon seizure of the SUBJECT DOMAIN NAMES by the FBI, Namecheap Inc. will be directed to associate the SUBJECT DOMAIN NAMES to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve indicating that the sites has been seized pursuant to a warrant issued by this court.

77. Because the warrant will be served on Namecheap Inc., which controls the SUBJECT DOMAIN NAMES, and Namecheap Inc., thereafter, at a time convenient to it, will transfer control of the SUBJECT DOMAIN NAMES to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

**REQUEST FOR SEALING**

78. It is additionally requested that this affidavit be filed under seal until further Order of the Court. In support of this request, your affiant states that the information contained in this affidavit and all related document, is part of a continuing criminal investigation. The targets of this investigation are likely not aware of the scope of this investigation, and of the information that has been gathered in this investigation. It is the opinion of your affiant that if this affidavit and related documents are made available for public viewing, it would seriously jeopardize the ongoing criminal investigation. Therefore, it is respectfully requested that this application, affidavit, exhibits, and inventory return be filed under seal, until further Order of the Court, except that copies of the warrants and attachments may be served at the time it is executed and the government may provide these documents, as required by its discovery obligations, including Rule 16 of the Federal Rules of Criminal Procedure.



---

JORDAN F. SLAVIK  
Special Agent  
Federal Bureau of Investigation

Affidavit for Seizure Warrants submitted electronically by email in .pdf format. Oath administered, and contents and signature, attested to me as true and accurate telephonically

pursuant to Fed.R.Crim. P. 4.1 and 41(d)(3) on November 15, 2024.

*H. Kenneth Schroeder, Jr.*

---

HONORABLE H. KENNETH SCHROEDER, JR.  
United States Magistrate Judge

**ATTACHMENT A-1: PROPERTY TO BE SEIZED**

Pursuant to this warrant, Binance shall effectuate the freeze/seizure of all cryptocurrencies stored within or associated with Binance User ID 19925727, including all First Digital USD, Bitcoin, Litecoin, Ethereum, TetherUS, BNB, NEO, Tokocrypto, and Gravity. Binance shall work to provide the frozen/seized property to the U.S. government in a reasonably practicable manner, provide reasonable assistance in implementing the terms of this seizure warrant, and take no unreasonable action to frustrate the implementation of it.

**ATTACHMENT A-2: PROPERTY TO BE SEIZED**

With respect to popeyetools.com, popeyetools.co.uk, and popeyetools.to (“SUBJECT DOMAIN NAMES”), Namecheap Inc., who is the domain registrar for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of SUBJECT DOMAIN NAMES:

1) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation (FBI), by associating the SUBJECT DOMAIN NAMES to the following authoritative name-server(s):

(a) ns1.fbi.seized.gov

(b) ns2.fbi.seized.gov

(c) Any new authoritative name server to be designated by a law enforcement agent in writing, including e-mail, to the Subject Registrar.

2) Prevent any further modification to, or transfer of, SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI.

3) Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.

4) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.



5) To the extent necessary and appropriate, the Government may display a notice on the websites to which the Subject Domain Names will resolve. Those notices will consist of law enforcement emblems and the following text (or substantially similar text):

“The domain has been seized by the Federal Bureau of Investigation and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Western District of New York as part of law enforcement action taken in parallel with the United Kingdom National Crime Agency.”